# Summary and Resources

## Summary and Resources

**Course Credit & Download page as a PDF**

for quick reference. For course credit, look for the "Feedback and Credit" button at the bottom of the page or go to our Credit SEC 0201 page now.

## Your Cyber Security Responsibility and Requirements

You're responsible for the cyber security of computers and devices that you use or manage - plus the information that is stored on them. Make sure that you meet our . Don't hesitate to contact your line manager, (password protected), or Cyber Security Operations at security@lbl.gov.

## Top threats: What to do and what not to do

| Top Threats | Do | Do not |
|---|---|---|
| Loss of PII | • If you see Personally Identifiable Information (PII) anywhere it does not belong, report it to security@lbl.gov<br>  • If you wish to report PII and remain anonymous, we can support that request<br>• If you work with PII, review our<br>• If you are involved in any process that may involve PII, contact security@lbl.gov and we'll help you develop the best controls and security<br>• Definition of PII: Social Security Number, Driver's License #, Financial Account Data, Individual identifier PLUS any type of health information | • Do not store PII on your computer, external hard drives, or mapped drives such as H: T: or V:<br>• Do not email PII.<br>• Do not store PII outside of HRIS or FMS, the institutional systems for human resources and financial data.<br>• Do not store paper collection of PII unless approved by Cyber Security Operations. |
| Spam and Phishing Attacks | • Report **targeted** spam or phishing to security@lbl.gov<br>• For normal spam or phishing (not targeted), use your email client to flag it as spam<br>• Verify web and email addresses (e.g. make sure it's a .gov, not .com)<br>• Be wary of vague messages or references to new or unknown projects<br>• When viewing an email think, "could this be an attack?" | • Do not open attachments you are not expecting<br>• Do not click on links in emails you are not expecting<br>• Do not provide your username or password or any other account information via email<br>• Do not download a file that ends in .exe |
| Drive-by Downloads | • Run the latest version of Chrome or FireFox<br>• PCs & Macs: Install BigFix on your work computer<br>• Set up auto updates for your operating system and applications when possible<br>• Install Antivirus software. Sophos is available for Berkeley Lab and home usage at software.lbl.gov | • Do not use Internet Explorer, except when required for business applications like FMS<br>• Do not ignore update notifications from your OS, browser, and third parties like Adobe<br>• Do not use old browser versions |

# Tools, Software, and Services

Throughout the course, we mention a variety of tools - here they are, all in one place. You can also visit  for more information and resources.

| Tool, Software, or Service | Description | Link to Resource(s) |
|---|---|---|
| BigFix | BigFix will automatically patch Java and Flash plugins for PCs and Macs (only use for your work computer). | • |
| Network blocks | Vulnerable computers are blocked from network access | • Check for blocks at |
| Sophos Anti-Virus | This is the cyber security team recommended Anti-Virus software. Available for Macs and PCs for work and home computers if used for work. | Download Sophos at . Look under the Security Software section. Installation instructions available here: |
| Change your Password Service | Use our password change service when required or when you have any reason to believe that your password has been compromised. | |
| Backup Services | Berkeley Lab offers a number of services for backing up data. | |
| Report theft of a mobile device | If any IT asset is lost or stolen, you should report it immediately using our form. | |
| Spirion | This software searches your computer to identify any potential PII. Available for PCs and Macs. | • Instructions on using Spirion:<br>• Download Spirion at . Look under the Security Software section. |
| Central Syslog | Macs and Linux/Unix systems must syslog to the central syslog server. **Exemption:** Do not syslog to the central syslog server if your computer is offsite or frequently offsite (e.g. a laptop). | Instructions for the central syslog: |

## Additional Training

| Training | Description | Link |
|---|---|---|
| **Privacy and Protected Information Training** | This training is required for employees that use or access PII. However, all employees are welcome to take it. | |
| **Social Engineering** | Spam and phishing rely on "social engineering" to trick you into clicking on that link or opening that bad attachment. You can read more about social engineering including other methods, e.g. telephone, media (CD's, DVD's, USB sticks), and the web. | |
| **Advanced training on Targeted Phishing** | In order to raise awareness of current phishing scam tactics, the Berkeley Lab Cyber Security team sends emails to Berkeley Lab employees that simulate real phishing attacks | |

## Policies & Procedures

You can read more about all cyber-related RPM policies and procedures at our .

**Download page as a PDF**

for quick reference.